Unicenter

NetMaster Network Management for TCP/IP Release and Migration Guide

Version 6.2

Computer Associates

The Software That Manages eBusiness

Booklist

June 02

Contents

Chapter 1: New Features of NetMaster for TCP/IP

Chapter 2: Migrating to NetMaster for TCP/IP 6.2

Chapter 1

New Features of NetMaster for TCP/IP

This chapter summarizes the new and enhanced features that are available in Unicenter NetMaster Network Management for TCP/IP Version 6.2 with Service Pack 3.0.

This chapter discusses the following:

What Is New in Service Pack 3.0

Service Pack 3.0 includes the following new and enhanced features in NetMaster for TCP/IP:

- Unicenter NetMaster Socket Management for CICS 1.0
- Unicenter NetMaster Reporter 2.0
- Connection list enhancements

Unicenter NetMaster Socket Management for CICS 1.0

NetMaster for TCP/IP provides an interface to NetMaster Socket Management for CICS. When this interface is enabled, it does the following:

- Passes additional CICS information about TCP connections to NetMaster for TCP/IP, such as user ID, CICS transaction name, and CICS transaction number.

  This information then becomes available through central network management displays within NetMaster for TCP/IP.
- Allows you to monitor CICS IP resources (resource class CICMON).

See the following for more information:

- *Unicenter NetMaster Socket Management for CICS Getting Started*
- Chapters "Managing Connections" and "Monitoring CICS Resources" in the *Unicenter NetMaster Network Management for TCP/IP User Guide*

NetMaster Reporter 2.0

With Service Pack 3.0, you can use Unicenter NetMaster Reporter 2.0 in NetMaster for TCP/IP 6.2. NetMaster Reporter is a network performance and analysis tool that provides:

- Web-based historical and trend reporting of collected data from TCP/IP activities
- An integrated and flexible report scheduler service
- Reports on demand
- Easy access to generated reports
- Data consolidation from multiple systems
- Mainframe installation and Web hosting

See the *Unicenter Working with NetMaster Reporter* guide for more information.

Connection List Enhancements

Service Pack 3.0 provides the following enhancements to connection lists:

- A new connection list menu from which you can list any of the following connection types:
  - Telnet
  - Telnet – with Response Times
  - Telnet – with Round Trip Times
  - CICS Socket
  - CICS Socket – with History
  - Connections
  - Connections – Fast
  - Connections – with History
- The ability to save and recall criteria for specific types of connection and to administer these criteria

See the chapters “Managing Connections” and “Monitoring CICS Resources” in the *Unicenter NetMaster Network Management for TCP/IP User Guide* for more information.

What Was New in Version 6.2

Version 6.2 included the following new and enhanced features:

- Initialization and Customization Services (ICS)
- Menu restructure, shortcuts, and tip of the day
- Logging enhancements
- IP resource monitor
- Express setup of resources
- Monitoring stack performance
- Monitoring and diagnosing multiple stacks from a single region
- Resource-based port monitoring
- Additional information on connection lists
- Alternative format for Device Links display for a stack
- Web enhancements
- Enhanced multisystem support
- Enhanced resource-based security

Initialization and Customization Services (ICS)

You now use Initialization and Customization Services (ICS) to customize your NetMaster for TCP/IP region. ICS is a computer-assisted initialization facility that enables you to implement a region rapidly and easily. Also, ICS enables you to customize parameters easily at a later stage.

When you first log on to a region, you need to set various parameters to get the product up and running. ICS helps you set up these parameters. An initial dialog is supplied for the first time user, to walk you through the process. You are prompted to supply required parameter values and given the opportunity to supply optional parameter values within various parameter groups.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *Management Services Release and Migration Guide.*

Menu Restructure, Shortcuts, and Tip of the Day

The user interface menus for NetMaster for TCP/IP and related products have been unified in such a way as to make their structure logical, intuitive, and easy to navigate. They also now include shortcuts to go directly to a function. Shortcuts are shown beside options on menus.

Selecting a Function Directly by Using Shortcuts

To jump to the panel of a function directly:

- Specify ***/shortcut-name*** to retain the current panel on return.
- Specify ***=/shortcut-name*** to close the current panel and return to the primary menu on exit.

Note: Enter **/** or **=/** to list all shortcuts.

Tip of the Day

Each time you log on to your NetMaster for TCP/IP region, the primary menu shows a tip of the day. To view more details of a tip, position your cursor on it and press F1 (Help).

Logging Enhancements

The activity log has been enhanced in the following ways:

- Supports multiple concatenated log files.
- Supports filtering by text, origin, or region.
- Text finding has been enhanced as follows:
  - Supports 'FIND text FIRST' and 'FIND text LAST' (within the current day).
  - Supports compound FIND arguments, using the AND (&) or OR (|) operators.
  - The scan limit can be set in the $NM LOGFILES parameter group in ICS.
- The DATE command and TIME commands support larger sets of operands. You can now position the log by either relative time or absolute time.
- Allows you to print parts of the log.
- Supports a user-written log exit.

For further information, see the *Management Services Administrator Guide.*

IP Resource Monitor

NetMaster for TCP/IP now supports an IP resource monitor, which enables you to:

- View the status of diverse resource types from a single integrated display.
- View performance information about your network
- Perform diagnostic functions on selected resources

The classes of IP resources that you can monitor are:

- ASMON—address spaces
- CIP—Cisco channel cards
- CSM—Communication Storage Manager
- EE—Enterprise Extender
- OSA—Open Systems Adapters and OSA Express
- ROUTER—IBM 2216 routers
- STACK—TCP/IP stacks

The IP resource monitor is now used for all diagnostic and monitoring functions for these resources, replacing the diagnostic menu options previously used.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide.*

Express Setup of Resources

NetMaster for TCP/IP now supports an express setup of resources. This option automatically creates resource definitions for IP resources that are configured on or accessible from the local region, so that you can implement your region as quickly as possible.

For further information, see the *NetMaster for TCP/IP Implementation Guide* and the *NetMaster for TCP/IP Administrator Guide.*

Monitoring Stack Performance

You can now monitor stack performance from the IP resource monitor by using the following commands:

- IP to view stack IP performance history
- IPM to view stack IP performance metrics

The same information is available on the web interface by selecting the following options from the OS/390 IP Stack Diagnostics page:

- View IP Performance History
- Display IP Performance Metrics

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide.*

Monitoring and Diagnosing Multiple Stacks from a Single Region

If you have multiple IP stacks on one OS/390 image, you can have visibility of all stacks from the IP resource monitor.

You can perform diagnostics and view performance information on all stacks from one NetMaster for TCP/IP region.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide.*

Resource-based Port Monitoring

You can now monitor one or more ports for an ASMON or STACK resource from the IP resource monitor.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide.*

Additional Information on Connection Lists

Connection lists now include additional information from the following sources:

- NetSpy
- SNMP

For further information, see the online help for the connection list panels.

Alternative Format for Device Links Display

You can now use the new DL command against a stack on the IP resource monitor to display a list of device links for the stack. You can then toggle between the list and the graphical display of device links to obtain the information that you require.

For further information, see the *NetMaster for TCP/IP User Guide*.

Web Enhancements

The web interface has been enhanced in the following ways:

- The 'Run a command' option now retains a command history, so that you can select a command from a dropdown list to reissue.
- The 'Command help' window displays help on command syntax.
- The 'Message help' window provides help on a message and allows you to type in a message ID or to move to the previous or next message.

For further information, see the web help for these pages.

Enhanced Multisystem Support

Enhanced multisystem support provides visibility of all defined local and remote resources on a single IP resource monitor.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide*.

Enhanced Resource-based Security

Resource-based security is now available in NetMaster for TCP/IP.

Resource-based security allows you to control a user's access to menus, resources, and commands.

For further information, see the *NetMaster for TCP/IP Administrator Guide* and the *NetMaster for TCP/IP User Guide*.

Summary of New Features in Version 6.1

NetMaster for TCP/IP Version 6.1 enabled you to use NetMaster Reporter 1.0, a network performance and analysis tool.

Summary of New and Enhanced Features in Version 6.0

SOLVE:Manage Version 6.0 included the following new and enhanced features:

- Connection awareness—to identify the stacks, applications, and users associated with your TCP/IP system
- Access control—to take control of your TCP/IP resources
- OSA support—to list the devices defined on an OSA, measure the traffic through an OSA, and map OSA traffic to the stack generating it
- INI file—if you have multiple systems, this feature removes the need to use the administration panels to initialize each system (now enhanced to ICS).
- Performance monitoring on:
  - Communication Storage Manager (CSM)
  - TCP/IP stacks
  - Address space
  - Enterprise Extender
  - OSAs
- Extensions to the web interface.
- Improvements to the menu structure.
- Improvements to the diagnostics.
- Alert monitor predefined filters and occurrence counter.

Summary of New and Enhanced Features in Version 5.0

SOLVE:Netmaster for TCP/IP Version 5.0 included the following new and enhanced features:

- Web browser user interface was enhanced to:
  - Manage IP nodes and connections
  - Diagnose 2216 routers, Cisco channel cards, and printers
  - Perform IBM TCP/IP diagnostics
  - Monitor alerts, IP nodes, and alert history
  - Monitor stack performance
  - View the history of alerts and apply actions
  - Use utilities to run commands, view the activity log, change your password, and log off
- Command and resource-based security
- Alert monitor filtering and formatting functions

Chapter 2

Migrating to NetMaster for TCP/IP 6.2

This chapter describes the tasks associated with migrating to Version 6.2 of NetMaster for TCP/IP.

This chapter discusses the following:

Management Services Minimum Maintenance Level

Version 5.0 is the minimum maintenance level of Management Services that NetMaster for TCP/IP 6.2 can operate with.

Management Services provides a central core of basic functions and services for this product.

Changes to Security Setup

Automation Services resource-based security is now available in NetMaster for TCP/IP, allowing you to control a user's access to menus, resources, and commands by using the Network Partitioning Facility (NPF) or a third-party security package, such as RACF.

NPF Control Tables

The NPF control tables for user profiles have now changed, as shown in the following table:

Users	Old NPF Table	New NPF Table
Help desk operators	$IPNPFHD	$RMSXMON
Administrators	$IPNPFAD	$RMSXADM
Network operators	$IPNPFNO	$RMSXNOP
Operators	n/a	$RMSXOPR

If any user definitions specify resource-based security, replace the old NPF table name in the UAMS definition. The NPF table name is specified in the NPF Resource List Member field.

NPF Command List Members

The NPF command list members that determine what functions are available have also now changed, as shown in the following table:

Users	Old NPF Command List Member	New NPF Command List Member
Help desk operators	$IPHDESK	$RMSX220
Administrators	$IPADMIN	$RMSX020
Network operators	$IPNETOP	$RMSX320
Operators	n/a	$RMSX120

If you have modified any of the old NPF command list members, you need to apply your changes to the new members.

Third-party Security Products

The security profiles that support third-party security products are shown in the following table:

Security Product	Security Profile
CA-ACF/2 earlier than Version 6.0	$RMSXACF
CA-ACF/2 Version 6.0 or later	$RMSXAC6
RACF	$RMSXRCF
CA-Top Secret earlier than Version 5.0	$RMSXTSS
CA-Top Secret Version 5.0 or later	$RMSXTS5

For further information about setting up security for users, see the *Automation Services Administrator Guide*.

Log File Compatibility

The physical format of the activity log files for all products has changed with Management Services 5.0. You can no longer use your old Management Services log files.

Note: There are no conversion utilities provided for converting old-format log files to the new format.

You can still browse activity logs across regions with different Management Services levels. From Management Services 5.0, you can browse the following types of activity logs in other regions:

- Management Services 4.0 or 4.1
- Automation Services 4.0

This browsing facility is available in both directions between regions.

Customized Log Procedures

$LOGPROC and $LOGBROW are now $LOPROC and $LOBROW respectively. You cannot customize $LOPROC or $LOBROW, because they are not written in Network Control Language (NCL).

If you have modified $LOGPROC, you need to write a log exit routine incorporating your changes.

For further information about log exits, see the *Management Services Administrator Guide*.

Migrating to Version 6.2

Important! *Before proceeding with your migration tasks, ensure that you have done the following:*

- Completed the installation and setup tasks described in the *Unicenter Mainframe Network Management Installation and Setup Instructions*
- Reviewed the migration tasks described in the *Management Services 5.0 Release and Migration Guide*

To migrate to Version 6.2 from Version 6.1, Version 6.0, or Version 5.0, perform the following tasks:

Note: Unless indicated, a migration task is applicable regardless of the version you are migrating from. If a migration task is version-specific, the task heading indicates the applicable version.

Task 1—Migrate IPFILE Resource Definitions

For this release, you need to migrate your TCP/IP resource definitions from your IPFILE to the knowledge base for your NetMaster for TCP/IP region.

To perform this migration, perform the following subtasks:

- Subtask 1.1—Copy the data from your current IPFILE to a new IPFILE
- Subtask 1.2—Migrate your new IPFILE

Subtask 1.1—Copy the Data from Your Current IPFILE to a New IPFILE

This subtask ensures that your non-RAMDB resources are included in your new IPFILE.

Use the Access Method Services (IDCAMS) REPRO function to copy the data from your current IPFILE to a new IPFILE.

Subtask 1.2—Migrate Your New IPFILE

This subtask ensures that those resources now stored on the RAMDB are migrated from your IPFILE.

To use the IP Resource Migration Utility to migrate your new IPFILE, do this:

1. Enter **/ASADMIN.MIP** at the ===> prompt. The Automation Services : IP Resource Migration Utility panel is displayed.
2. Enter values in the parameter fields, as follows:
   - In the IPFILE Dataset field, specify the dataset name of your new IPFILE (created in subtask 1.1) to be migrated.
   - In the Report Dataset field, specify the dataset name to be used for the migration utility report.
   - In the Report Volume and Unit fields, optionally specify the volume serial details for the migration utility report.
   - In the System Name and Version fields, specify the target system image name and version to hold the migrated resources. (You can enter **?** in the System Name field to display a selection list. When you select a value, the utility inserts it in both fields.)
   - In the Replace Duplicate? field, specify (YES or NO) whether to replace entries that have the same name as entries being migrated.
3. Press F6 (Action). The utility migrates your IP resources and produces a migration report.
4. When the migration is complete, check the migration report.
5. If the migration report shows any error, follow the instructions to correct the error.

Task 2—Migrate VFS File

You can migrate your existing VFS dataset to NetMaster for TCP/IP 6.2 so that you can use such things as report definitions or alert monitor filters that you have set up. However, the system parameters that you have set no longer apply; you need to set new parameters, using ICS.

See the *NetMaster for TCP/IP Implementation Guide* for details of specifying parameters.

Task 3—Clear the Web Browser Cache (Web Interface Only)

If you are using the web interface, it is recommended that you clear the cache of your web browser. This is to prevent your getting a mix of old and new web files.

The way to clear your web cache varies, depending on your web browser. Complete the appropriate one of the following subtasks:

- Subtask 3.1—Clear the Cache on Internet Explorer
- Subtask 3.2—Clear the Cache on Netscape Navigator

Subtask 3.1—Clear the Cache on Internet Explorer

To clear the cache on Internet Explorer, do this:

1. From the Tools Menu of Internet Explorer, choose Internet Options. The Internet Options dialog box is displayed.
2. Click the General tab.
3. In the Temporary Internet files section, click the Delete Files button. The Delete Files dialog box is displayed.
4. Click OK. The Internet Options dialog box is displayed.
5. Click OK to close the Internet Options dialog box.

Your browser cache is now cleared.

Subtask 3.2—Clear the Cache on Netscape Navigator

To clear the cache on Netscape Navigator, do this:

1. From the Edit Menu of Netscape Navigator, choose Preferences. The Preferences dialog box is displayed.
2. In the Advanced category, click the Cache option.
3. Click the Clear Memory Cache button, and then click OK in the Confirmation dialog box that is displayed.
4. Click the Clear Disk Cache button and then click OK in the Confirmation dialog box that is displayed.
5. Click OK to close the Preferences dialog box.

Your browser cache is now cleared.

Task 4—Set Up the Data Space (Version 5.0 Only)

For the connection awareness function to work properly, it must see the connection activity. If a connection starts before connection awareness has started, NetMaster for TCP/IP is not aware of it.

To ensure that your system is aware of all connections, start your data space before TCP/IP and NetMaster for TCP/IP in the system IPL sequence.

Task 5—Set Up IBM TCP/IP SMF and TCPaccess Exits (Version 5.0 Only)

The data space interfaces with:

- The IBM TCP/IP SMF exits
- The TCPaccess stack exits and the log message forwarding exit

The migration process for these exits is described in the following subtasks. You must set up the exits for each stack on your system.

Subtask 5.1—Set Up IBM TCP/IP SMF Exits

If you have IBM TCP/IP SMF exits, replace the installation and implementation members with the equivalent members distributed in Management Services Version 5.0. These are shown in the following table.

Function	Version 5.0 Member	Version 5.0 Library	Version 6.2 Member	Version 6.2 Library
SMF exit load	IPSMFEX	IPLOAD	NMSMFIBM	MSLOAD
SMF exit module source	IPSMFEX	IPSAMP	-	-
SMF exit macro	$IPSMFEX	IPMACROS	-	-
SMF exit JCL	IPSMFAL	IPSAMP	-	-
SMF exit definition	IPPROGXX	IPSAMP	NMPROGCS	*dsnpref*.MS500.BASE.INSTALL

The library names in the table relate to the DDDEF entry name of the target zone.

Note: The SMF exit load module, previously distributed in both source and object form, is now distributed in object (load module) form only. This module cannot be customized.

Important! *Do not have both IPSMFEX and NMSMFIBM in the same LPAR. Otherwise, duplicate SMF data will be delivered to your NetMaster for TCP/IP regions. If you are running both Version 5.0 and Version 6.2 on the same LPAR, use NMSMFIBM.*

To migrate to the new IBM SMF exit, do this:

1. Open your SYS1.PARMLIB(PROG*xx*) member and change the IPSMFEX exit registration statements to NMSMFIBM exit registration statements.
2. Register the new exit with the OS/390 SET command. For example:

   ```
   SET PROG=xx
   ```

   The new exit will be used after the next IPL.
3. Deregister the existing exits using the OS/390 SETPROG EXIT command. For example:

   ```
   SETPROG EXIT,DELETE,EN=exitname,MODNAME=IPSMFEX
   ```

   where *exitname* is:

   - SYS.IEFU83
   - SYS.IEFU84
   - SYS.IEFU85
   - SYSSTC.IEFU83
   - SYSSTC.IEFU84
   - SYSSTC.IEFU85

   and, if registered:

   - SYSTSO.IEFU83
   - SYSTSO.IEFU84
   - SYSTSO.IEFU85
   - SYSOMVS.IEFU83
   - SYSOMVS.IEFU84
   - SYSOMVS.IEFU85

Subtask 5.2—Set Up TCPaccess Stack Exits

If you have TCPaccess exits, replace the installation and implementation members with the equivalent members distributed in Management Services Version 5.0. These are shown in the following table.

Function	Version 5.0 Member	Version 5.0 Library	Version 6.2 Member	Version 6.2 Library
SMF exit load	IPSMFEX	IPLOAD	-	-
SMF exit module source	IPSMFEX	IPSAMP	-	-
SMF exit	$IPSMFEX	IPMACROS	-	-
SMF exit JCL	IPSMFAL	IPSAMP	-	-
SMF exit definition	IPPROGXX	IPSAMP	-	-
TCPaccess exit	NMTCPAXS	IPLOAD	NMDSPAXS	MSLOAD

Note: The TCPaccess exit, NMDSPAXS, replaces both the old TCPaccess exit (NMTCPAXS) and the SMF exit (IPSMFEX).

The library names in the table relate to the DDDEF entry name of the target zone.

To migrate to the new TCPaccess exit, do this:

1. If you have:
   - TCPaccess 5.2—apply either the SP0106 tape or the CUM0010 tape
   - TCPaccess 5.3—apply either the SP0106 tape or the CUM0102 tape

   These enable the TCPaccess exit to receive copies of SMF records.
2. Change the EXIT statement in your IJTCFG*xx* member from NMTCPAXS to NMDSPAXS.
3. Recycle TCPaccess.
4. Remove the IPSMFEX exit registration statements from your SYS1.PARMLIB(PROG*xx*) member.

5. Deregister the existing exits by using the OS/390 SETPROG EXIT command. For example:

   ```
   SETPROG EXIT,DELETE,EN=exitname,MODNAME=IPSMFEX
   ```

   where *exitname* is:

   - SYS.IEFU83
   - SYS.IEFU84
   - SYS.IEFU85
   - SYSSTC.IEFU83
   - SYSSTC.IEFU84
   - SYSSTC.IEFU85

   You might have only SYS.IEFU84 and SYSSTC.IEFU84 registered.

Note: The new NMDSPAXS exit is installed in the implementation phase. For more information, see the instructions in the *Unicenter NetMaster Network Management for TCP/IP Implementation Guide.*

Enabling the Alert Monitor Occurrence Counter

The alert monitor occurrence counter has the columns:

- First date/time
- Elapsed time
- Occurrences

If these are not included in your alert monitor display on the web interface, do this:

1. From the Web Main Menu, choose Monitoring, Alerts, and then click the **Options** button.

   The Advanced Option dialog box is displayed.

2. From the Available Fields Not in Use column select:

   - First date/time
   - Elapsed time
   - Occurrences

3. Click the **Add** button.

The three fields now appear in the Show Fields in Order column.

4. Click Save Settings. The alert monitor occurrence counter is now enabled.

Where to Next?

You have now completed your migration tasks. To implement NetMaster for TCP/IP, follow the instructions in the *Unicenter NetMaster Network Management for TCP/IP Implementation Guide.*